IJARIIT INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact Factor: 6.078
(Volume 7, Issue 2 - V7I2-1441)
Available online at: https://www.ijariit.com

Block-wise data hiding using an improved flipping algorithm for image steganography

Vishav Batra
batravishav@gmail.com
Adesh Institute of Engineering and Technology, Faridkot, Punjab

Sarabjeet Kaur
sarb7316@gmail.com
Adesh Institute of Engineering and Technology, Faridkot, Punjab

ABSTRACT

Image steganography algorithms hide the secret data in the cover image and gives the stego image in the output. The visual quality is degraded due to data hiding. In the literature, the flipping algorithm is the most preferred data hiding algorithm to reduce the variability. In this algorithm, the secret data is flipped if the variability between the cover and stego image is greater than 50%. In our work, we have enhanced this algorithm and designed an improved flipping algorithm. In the proposed algorithm, the cover image is processed in blocks and each block variability is determined. If the variability of the block is higher than the threshold value then-secret data is flipped and hide in the cover image. Thus, in the proposed algorithm, in some blocks, secret data is hidden in the original form and some blocks in flipped form. In the last, we have performed the experimental results on the standard dataset images and various parameters calculated. The result shows that the proposed algorithm enhances the visual quality of the cover image as compared to the existing algorithms. However, in the proposed algorithm need to communicate information with the receiver, the data is hidden in the original or flipped form.

Keywords: *Data Hiding, Flipping Algorithm, Steganography, Security.*

1. INTRODUCTION

The technique of hiding a secret message behind a cover media is called steganography [1]. Also, often referred to as hidden writing. With regard to encryption, the distinct and visible coded knowledge is more desirable to attackers because of its unbreakability. Steganography provides a viable solution to encoding in oppressive regimes, which could attract undue scrutiny using cryptography [2]. Classical steganography refers to means for hidden correspondence, primarily in Cardan grille, invisible ink, Tibetan poetry, etc., used by people in ancient times. Modern steganography involves using computer and interactive networking technologies to mask the message in digital media. The two basic components of a modern steganographic method are embedding and extracting algorithms. There are two inputs accepted from the embedding algorithm: the hidden data and the cover image used for the message. The resultant image is known as the stego image. The stego image is also shown as an input to the hidden message extraction algorithm to extract the original secret data. Many covering items, including text, image, audio, and video, are available in the literature [3]. Image is the most common cover object. There are several pixels in the image. So, the hidden data in the cover image is challenging to threaten.

In the literature, numerous data hiding algorithm is available. The most preferred algorithm is the LSB algorithm in which the cover image LSB bit is replaced with secret data [4] bit. However, it simple and prone to attacks. Further, an edge-based data hiding algorithm is proposed in which cover image edges are determined and data hide in it using the K-bit LSB algorithm [5]. It provides better security but very less capacity as compared to the LSB algorithm. Next, flipped-based data hiding algorithms are proposed in which secret data is flipped before data hiding to improve the security [6]. However, this algorithm has not reduced the variability. Therefore, in order to reduce the variability, a flipped algorithm is proposed by Astuti et al. [7] in which secret data is flipped if the variability in the cover image is greater than 50% after data hiding. However, this algorithm is applied to the entire image. Thus, a very little bit of variability was reduced. In our work, we have taken this paper under consideration and designed an improved flipping algorithm that processes the cover image into blocks and measures the variability of the blocks. According to the block variability, data is hidden in the flipped or original form.

The main contribution of this paper is to design an algorithm that provides lesser variability without degrading the embedding capacity. To achieve this goal, we have designed an improved flipping algorithm. The improved flipping algorithm measures the variability between the cover image after data hiding. If the variability is greater than 50% then data is flipped else data hide in the original form. In addition, the cover image is processed in blocks. Thus, in some blocks data hide in the flipped form, and in some blocks in the original form that enhances the security because only the transmitter and receiver know data is hidden in the original or flipped form. The experimental results show that the improved flipping algorithm provides better PSNR as compared to the existing algorithm.

The rest of the paper is as follows. Section 2 gives an overview of the existing LSB and flipping algorithm. Section 3 illustrates the improved flipping algorithm. Section 4 shows the experimental results for the improved flipping algorithm and its comparative analysis with the existing algorithms. In section 5, a conclusion is drawn.

2. RELATED WORK

In this section, to understand the problem for the proposed algorithm, the LSB algorithm and flipped algorithm is explained with an example.

2.1 LSB Algorithm

In the spatial domain, the least significant bit (LSB) is the most preferred algorithm. The main motive of the LSB algorithm is to conceal the secret data into the cover image. The LSB-based data hiding is shown in Figure 1 [8]. To understand the LSB algorithm, it is explained with an example. Let the secret data have 8 bits and the cover image has 8 pixels. To achieve the data hiding using the LSB algorithm, the LSB bit of the cover image is replaced with the data bit. Thus, each pixel of the cover image pixel carries one bit of the secret data. After data hiding, a stego image is obtained on the output side. On the receiver side, the stego image read. After that, each pixel LSB bit is extracted to recover the original secret data.

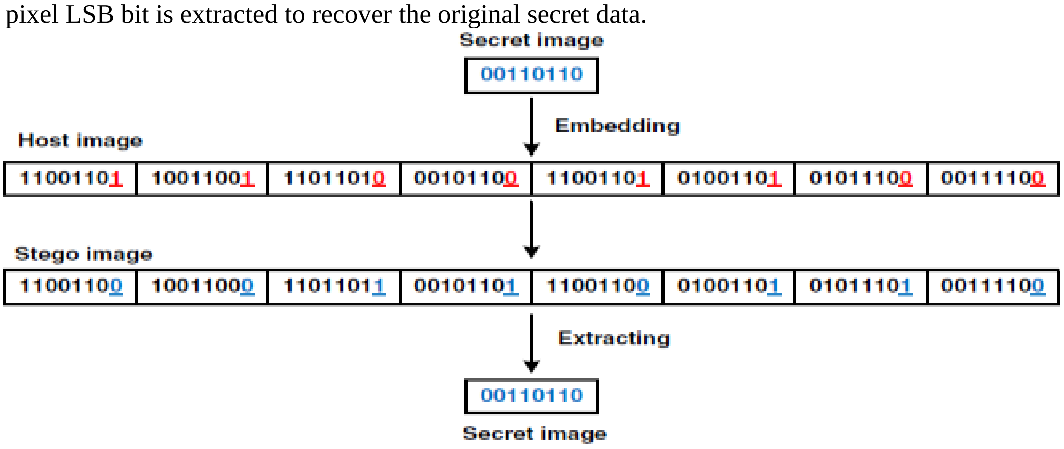


Fig. 1: LSB Algorithm

2.2 Flipped Algorithm

In the flipping method, the secret data is flipped before data hiding. An example of flipping method is shown in Figure 2. Let, the secret data is 10010010. The flip method complements the secret data and changed it into 01101101 [6].

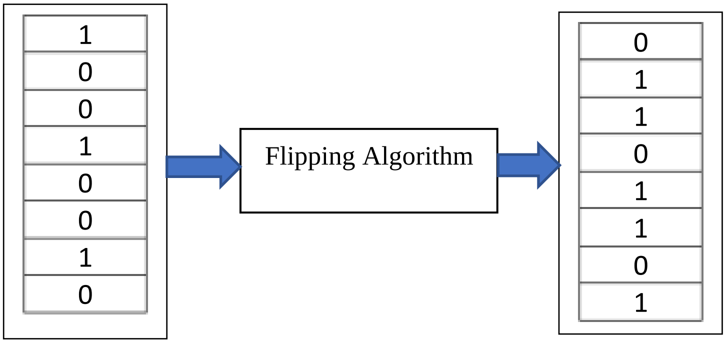


Fig. 2: Flipping Algorithm

2.3 Motivation

Based on the study and analysis, we found the following challenges of LSB and flipping algorithm.

- The LSB algorithm provide high variability if the bits are not matched between cover and secret data bits.
- The flipping algorithm is not reduced the variability if the appropriate condition is determined.

These challenges are taken under consideration and we have designed a block-wise improved flipping algorithm that lesser variability and security, as explained below.

3. PROPOSED ALGORITHM

The proposed algorithm provides lesser variability as compared to the existing algorithm. In the proposed algorithm, the cover image is processed into blocks. The data hiding for one block is shown in Figure 3. Initially, the cover image block and secret data read. After that, hide the data in the cover image block using the LSB algorithm that gives stego image block in the output. Then, the absolute difference between the cover block and the stego block is calculated using Eq. (3.1). If the absolute difference is higher than the threshold value then-secret data is flipped and hide using the LSB algorithm. The threshold value is calculated using Eq. (3.2).

$$AD = sum(|CB - SB|) \qquad (3.1)$$

$$T = \frac{\text{Maximum Difference between CB and SB}}{2} \qquad (3.2)$$

Where AD, T denotes the absolute difference and threshold. On the other side, CB, SB denotes the cover block and stego block.

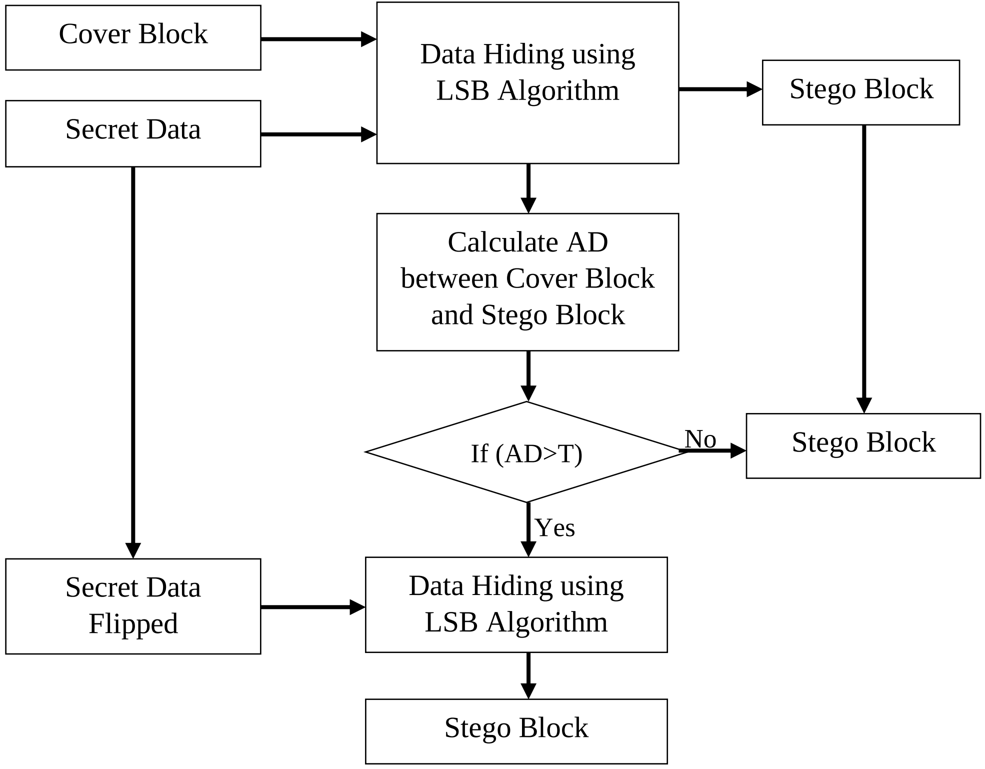

Cover Block
Secret Data
Data Hiding using LSB Algorithm
Stego Block
Calculate AD between Cover Block and Stego Block
If (AD>T)
No
Stego Block
Yes
Secret Data Flipped
Data Hiding using LSB Algorithm
Stego Block

Fig. 3: Block Diagram of the Proposed Algorithm for One Block

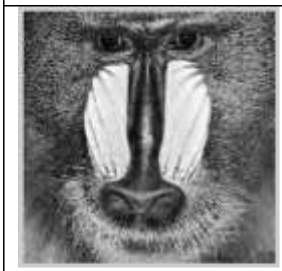
4. EXPERIMENTAL RESULTS

This section presents the experimental results carried out for the proposed algorithm to validate its performance against existing algorithms. The standard dataset images were downloaded from USC-SIPI Image Dataset [9]. The secret data is randomly generated. The algorithm is written and simulated in MATLAB and measure various performance parameters.

4.1 Visual Quality Analysis

In this analysis, based on the visual quality, the cover and stego images are compared. Table 1 shows the comparative analysis based on the visual quality with the existing algorithms. The results show that the proposed method looks similar to original images.

Table 1 Comparative Analysis based on the Visual Quality with the Existing Algorithms

Original Images	LSB Algorithm [4]	Astuti et al. [7]	Improved Flipping Algorithm
 Lena			
 Baboon			

 Barbara			
 Pepper			
 Female			

4.2 Mean Square Error (MSE): This parameter measures the variability generated in the cover image due to data hiding [10]. It is calculated using Eq. (1).

$$MSE = \frac{1}{AB}\sum_{i=1}^{A}\sum_{j=1}^{B}(C_{ij} - S_{ij})^2 \qquad (1)$$

where AB denotes the row and columns of the cover image. *CS* denotes the cover and stego images. The results for the proposed algorithm are shown in Table 2. The result shows that the improved flipping algorithm provides lesser MSE as compared to the existing algorithms.

Table 2: Comparative Analysis based on the MSE with the Existing Algorithms

Images	LSB Algorithm [4]	Astuti et al. [7]	Improved Flipping Algorithm
Lena	0.2507	0.2503	0.2491
Baboon	0.2507	0.2507	0.2495
Barbara	0.2496	0.2481	0.2478
Pepper	0.2416	0.2416	0.2413
Female	0.2468	0.2468	0.2460

4.3 Peak Signal to Noise Ratio (PSNR): PSNR parameter measured the quality of stego image after data embedding [10]. It is calculated as (2)

$$\text{PSNR}=10\log_{10}\frac{P^2}{MSE}\,(\text{dB}) \qquad (2)$$

Here, P defined the maximum intensity and its value is 255 and MSE denotes the Mean Square Error. Table 3 shows the PSNR for different cover images. The results show that the improved flipping algorithm provides better PSNR as compared to the existing algorithms.

Table 3: Comparative Analysis based on the PSNR (in dB) with the Existing Algorithms

Images	LSB Algorithm [4]	Astuti et al. [7]	Improved Flipping Algorithm
Lena	54.1396	54.1460	54.1670
Baboon	54.1398	54.1398	54.1595
Barbara	54.1586	54.1853	54.1891
Pepper	54.3006	54.3006	54.3046
Female	54.2081	54.2081	54.2218

4.4 Embedding Capacity: This parameter shows how many bits hide in the cover image. It is calculated using Eq. (3). It is measured in bits per pixel (bpp). Table 4 shows that the proposed algorithm provides similar embedding capacity.

$$Ec = \frac{Number\ of\ bits\ hidden\ in\ the\ cover\ image}{Row \times Col} \qquad (3)$$

Table 4: Comparative Analysis based on the Embedding Capacity (in bpp) with the Existing Algorithms

Images	LSB Algorithm [4]	Astuti et al. [7]	Improved Flipping Algorithm
Lena	1	1	1
Baboon	1	1	1
Barbara	1	1	1
Pepper	1	1	1
Female	1	1	1

5. CONCLUSION AND FUTURE WORK

In this paper, an improved flipping algorithm is designed that provides lesser variability without degrading the embedding capacity. In order to achieve this goal, the cover image is processed in blocks. Each block variability is measured after data hiding if the variability in it greater than 50% after data hiding is done in flipped form else in the original form. The experimental results were performed on the standard dataset images and found that the proposed algorithm provides lesser MSE, better PSNR, and the same embedding capacity as compared to the existing algorithms. In the future, to enhance to the security and robustness, cryptography and error correction code are hybrid with the proposed method.

6. REFERENCES

[1] Liu, J., Ke, Y., Zhang, Z., Lei, Y., Li, J., Zhang, M., & Yang, X. (2020). Recent Advances of Image Steganography with Generative Adversarial Networks. *IEEE Access*, *8*, 60575-60597.

[2] Lu, X., Wang, Y., Huang, L., Yang, W., & Shen, Y. (2016, September). A secure and robust covert channel based on secret sharing scheme. In *Asia-Pacific Web Conference* (pp. 276-288). Springer, Cham.

[3] Alyousuf, F. Q. A., Din, R., & Qasim, A. J. (2020). Analysis review on spatial and transform domain technique in digital steganography. *Bulletin of Electrical Engineering and Informatics*, *9*(2), 573-581.

[4] Hussain, M., Wahab, A. W. A., Idris, Y. I. B., Ho, A. T., & Jung, K. H. (2018). Image steganography in spatial domain: A survey. *Signal Processing: Image Communication*, *65*, 46-66.

[5] Yang, C. H., Weng, C. Y., Wang, S. J., & Sun, H. M. (2008). Adaptive data hiding in edge areas of images with spatial LSB domain systems. *IEEE Transactions on Information Forensics and Security*, *3*(3), 488-497.

[6] Sahu, A. K., Swain, G., & Babu, E. S. (2018). Digital image steganography using bit flipping. *Cybernetics and Information Technologies*, *18*(1), 69-80.

[7] Astuti, E. Z., Setiadi, D. R. I. M., Rachmawanto, E. H., Sari, C. A., & Sarker, M. K. (2020, March). LSB-based bit flipping methods for color image steganography. In *Journal of Physics: Conference Series* (Vol. 1501, No. 1, p. 012019). IOP Publishing.

[8] Banharnsakun, A. (2018). Artificial bee colony approach for enhancing LSB based image steganography. *Multimedia Tools and Applications*, *77*(20), 27491-27504.

[9] http://sipi.usc.edu/database/

[10] Alia, A. S., Al-Tamimib, M. S. H., & Ahmed, A. (2020). Secure Image Steganography Through Multilevel Security. *Image*, *11*(1).